Claims

What is claimed is:

1. A method for charging a smart battery, the method comprising:

receiving an encrypted random string, wherein the encrypted random string includes a random string in an encrypted form;

decrypting the encrypted random string to recover the random string; and

transferring the random string to a device to authenticate the smart battery for the charging, the device being electrically coupled to the smart battery.

2. The method of claim 1, wherein the receiving comprises:

generating a random string, the random string being generated by the device;

encrypting the random string, the random string being encrypted with an encryption key included in the device to generate the encrypted random string;

transferring the encrypted random string, the encrypted random string being transferred from the device to the smart battery.

3. The method of claim 2, wherein the decrypting requires the encryption key.

4. The method of claim 2, wherein the encryption key is a private key.

5. The method of claim 2, wherein the encrypted form is defined by the device and includes the encryption key to encrypt the random string.

6. The method of claim 2, wherein the encryption key is at least 8 bits.

7. The method of claim 2, wherein the generating, encrypting and transferring is performed by a controller included in the device, wherein the device is included in an information handling system.

8. The method of claim 1, wherein the device authenticates the smart battery by verifying the random string is unchanged.

9. The method of claim 8, wherein the device identifies the smart battery as a counterfeit when the random string is changed, wherein the device disables the charging of the counterfeit.

10. The method of claim 1, wherein the encrypted form is defined by the device and includes an encryption key to encrypt the random string.

11. The method of claim 1, wherein the random string is alpha numeric.

12. The method of claim 1, wherein the random string is a random number.

13. The method of claim 1, wherein the transferring of the random string is via an SMBus.

14. A method for authenticating a smart battery, the method comprising:

generating a first random string, the first random string being generated by a device electrically coupled to the smart battery;

encrypting the first random string, the first random string being encrypted with a first encryption key included in the device to generate the encrypted first random string;

transferring the encrypted first random string, the encrypted first random string being transferred from the device to the smart battery;

decrypting the encrypted first random string with the first encryption key to recover a second random string;

encrypting the second random string, the second random string being encrypted with a second encryption key included in the smart battery to generate the encrypted second random string;

transferring the encrypted second random string, the encrypted second random string being transferred from the smart battery to the device;

decrypting the encrypted second random string with the second encryption key to recover the second random string; and

verifying the first random string and the second random string match to authenticate the smart battery.

15. The method of claim 14, wherein each of the first and second encryption keys is a private key.

16. The method of claim 14, wherein each of the first and second encryption keys is at least 8 bits.

17. The method of claim 14, wherein each of the first and second random strings is a random number.

18. A smart battery authentication system comprising:

a smart battery, wherein the smart battery includes:

a smart electronics operable to:

receive an encrypted random string, wherein the encrypted random string includes a random string in an encrypted form;

decrypt the encrypted random string to recover the random string; and

transfer the random string to a controller to authenticate the smart battery;

a communications bus for electrically coupling the smart electronics to the controller; and

the controller operable to authenticate the smart battery by generating the random string, generating the encrypted random string and verifying the random string is unchanged.

19. The system of claim 18, wherein the encrypted form is defined by the controller and includes an encryption key to encrypt the random string.

20. The system of claim 18, wherein the random string is a random number.

21. An information handling system comprising:

a processor;

a system bus;

a memory coupled to the processor through the system bus;

a power supply system operable to provide power to the processor, the bus and the memory, the power supply system being connectable to an AC adapter for deriving power from an AC power source;

a controller coupled to the processor and memory through the system bus, the controller operable to control the power supply system; and

wherein the power supply system includes:

a smart battery having a smart electronics, the smart electronics being operable to:

receive an encrypted random string, wherein the encrypted random string includes a random string in an encrypted form;

decrypt the encrypted random string to recover the random string; and

transfer the random string to the controller to authenticate the smart battery.

22. The system of claim 21, wherein the controller is operable to authenticate the smart battery by generating the random string, generating the encrypted random string and verifying the random string is unchanged.